What is claimed is:

1. An IDS log analysis support apparatus comprising:

a log collection section that collects a log of an intrusion detection system that is connected to a telecommunication network;

a database that stores and manages logs collected by the log collection section; and

a log analysis section that obtains statistics of the logs managed by the database and analyses the statistics.

2. The IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises an internal and external similarity analysis device that sequentially compares an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, with an outward log in the logs, which is a log of accesses made from the protected subject side to the non-protected subject side, and sequentially calculates a degree of similarity that shows an extent to which the inward log and the outward log match based on the result of the comparison, and determines whether or not an abnormality has occurred based on the degree of similarity.

3. The IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises an access country analysis device that, taking as a subject to be detected a name of a country to which belongs a transmission source of an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system,

allocates a ranking to occurrence frequencies of country names, and determines that an abnormality has occurred when there is a change in the ranking of the country names that are normally detected.

4. The IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises an access country analysis device that, taking as a subject to be detected a name of a country to which belongs a transmission source of an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, determines that an abnormality has occurred when there is an increase in the occurrence frequency of a country name that is not normally detected.

5. The IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises an access country analysis device that, taking as a subject to be detected a name of a country to which belongs a transmission destination of an outward log in the logs, which is a log of accesses made from a protected subject side of the intrusion detection system to a non-protected subject side of the intrusion detection system, allocates a ranking to occurrence frequencies of country names, and determines that an abnormality has occurred when there is a change in the ranking of the country names that are normally detected.

6. The IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises an access country analysis device that, taking as a subject to be detected a name of a country to which belongs a transmission destination of an outward log, which is a log of accesses made from a protected subject side of the

intrusion detection system to a non-protected subject side of the intrusion detection system that are in the logs, determines that an abnormality has occurred when there is an increase in the occurrence frequency of a country name that is not normally detected.

7. The IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises a ratio analysis device that compares a short term number of events, which is the number of a predetermined event contained in a predetermined unit time period in the logs, with an average value of a short term number of events for a plurality of the unit time periods, and determines whether or not an abnormality has occurred based on a ratio of the short term number of events relative to the average value.

8. The IDS log analysis support apparatus according to claim 1, wherein the log analysis section comprises a threshold learning device that calculates a short term number of events, which is the number of a predetermined event contained in a predetermined unit time period in the logs, and an average value of a short term number of events for a plurality of the unit time periods, and a standard deviation value of a short term number of events for a plurality of the unit time periods, and determines whether or not an abnormality has occurred using a result obtained by dividing a difference between the short term number of events of a subject being investigated and the average value by the standard deviation value.

9. The IDS log analysis support apparatus according to claim 1, wherein a plurality of intrusion detection systems are connected to the telecommunication network, and the plurality of intrusion detection systems each have a different protected subject, and the log analysis section comprises an IDS comparison device that compares a monitored

profile, which is characteristics of logs of a monitored intrusion detection system, which is one intrusion detection system from among the plurality of intrusion detection systems, with an integrated profile, which is characteristics of logs of all the intrusion detection systems other than the monitored intrusion detection system from among the plurality of intrusion detection systems, and determines that an abnormality has occurred when the difference between the monitored profile and the integrated profile is equal to or greater than a predetermined value.

10. The IDS log analysis support apparatus according to claim 9, wherein the IDS comparison device comprises a variable state comparison device that compares a variable state that accompanies an elapsed time of the monitored profile with a variable state that accompanies an elapsed time of the integrated profile, and determines that an abnormality has occurred when the difference between the variable states is equal to or greater than a predetermined value.

11. An IDS log analysis support method comprising the steps of:

regularly collecting a log of an intrusion detection system that is connected to a telecommunication network;

storing logs in a database and managing the logs; and

obtaining statistics of the logs managed by the database and performing analysis processing on the statistics.

12. The IDS log analysis support method according to claim 11, wherein the analysis processing comprises internal and external similarity analysis processing that sequentially compares an inward log in the logs, which is a log of accesses made from a

non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, with an outward log in the logs, which is a log of accesses made from the protected subject side to the non-protected subject side, and determines whether or not an abnormality has occurred using a degree of similarity that shows an extent to which the inward log and the outward log match based on the results of the comparison.

13. The IDS log analysis support method according to claim 11, wherein the analysis processing comprises access country analysis processing that sequentially detects an occurrence frequency of a name of a country to which belongs a transmission source of an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, allocates a ranking to occurrence frequencies of country names, and determines that an abnormality has occurred when there is a change in the ranking of the country names that are normally detected.

14. The IDS log analysis support method according to claim 11, wherein the analysis processing comprises access country analysis processing that sequentially detects an occurrence frequency of a name of a country to which belongs a transmission source of an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, and determines that an abnormality has occurred when there is an increase in the occurrence frequency of a country name that is not normally detected.

15. The IDS log analysis support method according to claim 11, wherein the analysis

processing comprises access country analysis processing that sequentially detects an occurrence frequency of a name of a country to which belongs a transmission destination of an outward log in the logs, which is a log of accesses made from a protected subject side of the intrusion detection system to a non-protected subject side of the intrusion detection system, allocates a ranking to occurrence frequencies of country names, and determines that an abnormality has occurred when there is a change in the ranking of the country names that are normally detected.

16. The IDS log analysis support method according to claim 11, wherein the analysis processing comprises access country analysis processing that sequentially detects an occurrence frequency of a name of a country to which belongs a transmission destination of an outward log in the logs, which is a log of accesses made from a protected subject side of the intrusion detection system to a non-protected subject side of the intrusion detection system, and determines that an abnormality has occurred when there is an increase in the occurrence frequency of a country name that is not normally detected.

17. The IDS log analysis support method according to claim 11, wherein the analysis processing comprises ratio analysis processing that sequentially calculates a ratio between a short term number of events, which is the number of a predetermined event contained in a predetermined time period in the logs, and a long term number of events, which is the number of the predetermined event contained in a time period that is longer than the predetermined time period, and determines whether or not an abnormality has occurred based on the ratio.

18. The IDS log analysis support method according to claim 11, wherein the analysis

processing comprises threshold learning analysis processing that calculates a short term number of events, which is the number of a predetermined event contained in a predetermined unit time period in the logs, and an average value of a short term number of events for a plurality of the unit time periods, and a standard deviation value of a short term number of events for a plurality of the unit time periods, and determines whether or not an abnormality has occurred using a result obtained by dividing a difference between the short term number of events of a subject being investigated and the average value by the standard deviation value.

19. The IDS log analysis support method according to claim 11, wherein a plurality of intrusion detection systems are connected to the telecommunication network, and the plurality of intrusion detection systems each have a different protected subject, and the analysis processing comprises IDS comparison processing that compares a monitored profile, which is characteristics of logs of a monitored intrusion detection system, which is one intrusion detection system from among the plurality of intrusion detection systems, with an integrated profile, which is characteristics of logs of all the intrusion detection systems other than the monitored intrusion detection system from among the plurality of intrusion detection systems, and determines that an abnormality has occurred when the difference between the monitored profile and the integrated profile is equal to or greater than a predetermined value.

20. The IDS log analysis support method according to claim 19, wherein the IDS comparison processing comprises variable state comparison processing that compares a variable state that accompanies an elapsed time of the monitored profile with a variable state that accompanies an elapsed time of the integrated profile, and determines that an

abnormality has occurred when the difference between the variable state is equal to or greater than a predetermined value.

21. An IDS log analysis support program that analyzes a log of an intrusion detection system connected to a telecommunication network, the IDS log analysis support program executing on a computer:

a log collection step in which logs are collected from the intrusion detection system;

a database creation step in which the logs collected in the log collection step are stored and the stored logs are managed; and

a log analysis step in which statistics are obtained for the logs managed in the database creation step and the statistics are analyzed.

22. The IDS log analysis support program according to claim 21, wherein the log analysis step comprises an internal and external similarity analysis step that sequentially compares an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, with an outward log in the logs, which is a log of accesses made from the protected subject side to the non-protected object side, and determines whether or not an abnormality has occurred using a degree of similarity that shows an extent to which the inward log and the outward log match based on the result of the comparison.

23. The IDS log analysis support program according to claim 21, wherein the log analysis step comprises an access country analysis step that sequentially detects an

occurrence frequency of a name of a country to which belongs a transmission source of an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, allocates a ranking to occurrence frequencies of country names, and determines that an abnormality has occurred when there is a change in the ranking of the country names that are normally detected.

24. The IDS log analysis support program according to claim 21, wherein the log analysis step comprises an access country analysis step that sequentially detects an occurrence frequency of a name of a country to which belongs a transmission source of an inward log in the logs, which is a log of accesses made from a non-protected subject side of the intrusion detection system to a protected subject side of the intrusion detection system, and determines that an abnormality has occurred when there is an increase in the occurrence frequency of a country name that is not normally detected.

25. The IDS log analysis support program according to claim 21, wherein the log analysis step comprises an access country analysis step that sequentially detects an occurrence frequency of a name of a country to which belongs a transmission destination of an outward log in the logs, which is a log of accesses made from a protected subject side of the intrusion detection system to a non-protected subject side of the intrusion detection system, allocates a ranking to occurrence frequencies of country names, and determines that an abnormality has occurred when there is a change in the ranking of the country names that are normally detected.

26. The IDS log analysis support program according to claim 21, wherein the log

analysis step comprises an access country analysis step that sequentially detects an occurrence frequency of a name of a country to which belongs a transmission destination of an outward log in the logs, which is a log of accesses made from a protected subject side of the intrusion detection system to a non-protected subject side of the intrusion detection system, and determines that an abnormality has occurred when there is an increase in the occurrence frequency of a country name that is not normally detected.

27. The IDS log analysis support program according to claim 21, wherein the log analysis step comprises a ratio analysis step that sequentially calculates a ratio between a short term number of events, which is the number of a predetermined event contained in a predetermined time period in the logs, and a long term number of events, which is the number of the predetermined event contained in a time period that is longer than the predetermined time period, and determines whether or not an abnormality has occurred based on the ratio.

28. The IDS log analysis support program according to claim 21, wherein the log analysis step comprises a threshold learning analysis step that calculates a short term number of events, which is the number of a predetermined event contained in a predetermined unit time period in the logs, and an average value of a short term number of events for a plurality of the unit time periods, and a standard deviation value of a short term number of events for a plurality of the unit time periods, and determines whether or not an abnormality has occurred using a result obtained by dividing a difference between the short term number of events of a subject being investigated and the average value by the standard deviation value.

29. The IDS log analysis support program according to claim 21, wherein a plurality of the intrusion detection systems are connected to the telecommunication network, and the plurality of intrusion detection systems each have a different protected subject, and the log analysis step comprises an IDS comparison step that compares a monitored profile, which is characteristics of logs of a monitored intrusion detection system, which is one intrusion detection system from among the plurality of intrusion detection systems, with an integrated profile, which is characteristics of logs of all the intrusion detection systems other than the monitored intrusion detection system from among the plurality of intrusion detection systems, and determines that an abnormality has occurred when the difference between the monitored profile and the integrated profile is equal to or greater than a predetermined value.

30. The IDS log analysis support program according to claim 29, wherein the IDS comparison step comprises a variable state comparison step that compares a variable state that accompanies an elapsed time of the monitored profile with a variable state that accompanies an elapsed time of the integrated profile, and determines that an abnormality has occurred when the difference between the variable states is equal to or greater than a predetermined value.